



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON DC 20350-2000

OPNAVINST 3030.5C
N3N5
22 Apr 2019

OPNAV INSTRUCTION 3030.5C

From: Chief of Naval Operations

Subj: NAVY CONTINUITY OF OPERATIONS PROGRAM AND POLICY

Ref: (a) Presidential Policy Directive 40 (PPD 40), National Continuity Policy
(b) Federal Continuity Directive of 1 January 2017
(c) DoD Directive 3020.26 of 14 February 2018
(d) SECNAVINST 3030.4D
(e) Federal Continuity Directive of 2 July 2013
(f) SECNAVINST 3501.1D
(g) DoD Instruction 6055.17 of 13 February 2017
(h) DoD Instruction 3020.42 of 17 February 2006
(i) OPNAVINST 3502.8
(j) DoD Instruction 8500.01 of 14 March 2014
(k) SECNAVINST 12271.1
(l) SECNAV M-5210.1 of January 2012
(m) Defense Continuity Program (DCP) Security Classification Guide, 15 December 2005
(n) 2018 Chairman of the Joint Chiefs of Staff Mission Assurance Benchmarks
(NOTAL)

Encl: (1) Policy
(2) Responsibilities
(3) COOP Program Minimum Requirements
(4) COOP Plan Assessment Benchmarks

1. Purpose

a. To establish policy, assign responsibilities, and specify requirements for implementing the Navy continuity of operations (COOP) program per guidance contained in references (a) through (n).

b. This revision updates COOP cybersecurity planning elements and provides a COOP plan assessment template. This is a complete revision and should be reviewed in its entirety.

2. Cancellation. OPNAVINST 3030.5B.

3. Scope and Applicability. This instruction applies to the Offices of the Chief of Naval Operations (OPNAV) and all Navy echelon 1 through echelon 6 commands.

4. Background

a. Per reference (a), it is the policy of the United States to maintain a comprehensive continuity capability at all levels of government to meet the essential defense and domestic needs of the Nation's citizens during periods of national emergency. As described in reference (b), COOP is an organization's ability to continue mission-essential functions (MEF) with little or no interruption during and in the aftermath of an emergency. In today's asymmetric environment, the Navy must plan and prepare to continue its MEFs under all circumstances and across the spectrum of threats, including natural disasters, and technological, pandemic, and man-made emergencies per reference (c).

b. The Navy COOP Program represents an integrated set of policies, plans, and procedures that support the Defense Continuity Program. The changing threat environment, recent emergencies, cyber vulnerabilities, and increased potential for terrorist use of weapons of mass destruction highlights the need for cohesive and coherent COOP capabilities.

5. Policy. Natural and man-made events can occur without warning causing disruptions to normal operations. The purpose of the Navy COOP Program is to ensure the ability of each organization to continue execution of its MEFs. COOP program policy is in enclosure (1).

6. Responsibilities. Every command and organization within the Department of the Navy (DON) will implement a COOP program unless their COOP planning is included in their next highest authority in their chain of command. COOP programs require the identification of MEFs and the development of COOP plans and procedures to provide continuity of MEFs under all circumstances across the spectrum of threats, disasters, or incidents. Responsibilities for the DON COOP program are in enclosure (2).

7. Discussion

a. COOP planning includes preparatory measures, response actions, and restoration activities planned or taken to ensure continuation of MEFs to maintain military effectiveness, readiness, and survivability. COOP planning is a good business practice, a part of the fundamental mission of the Navy and, as such, it should be incorporated into daily operations and activities. The minimum COOP planning elements are provided in enclosure (3).

b. COOP planning is best achieved through integration with the various programs under mission assurance that enable operational capability to continue with limited or no impact to mission execution, should an event or other disruption occur. Organizations and installations should develop integrated solutions among all programs that most effectively and efficiently enhance mission execution. A COOP assessment template is provided in enclosure (4).

8. Waiver. Waiver authority for this instruction is held by the Deputy Chief of Naval Operations for Operations, Plans and Strategy (CNO N3N5).

9. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the DON/Assistant for Administration, Directives and Records Management Division portal page at <https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx>.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact the local records manager or the DON/Assistant for Administration Directives and Records Management Division program office.

10. Review and Effective Date. Per OPNAVINST 5215.17A, CNO N3N5 will review this instruction annually on the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, Department of Defense (DoD), Secretary of the Navy (SECNAV), and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

11. Information Management Control. Data collection contained in the instruction is exempt from information management control per SECNAV M-5214.1 of December 2005, part IV, subparagraph 7l.



S. B. MUNSCH
Deputy Chief of Naval Operations
for Operations, Plans and Strategy

Releasability and distribution:

This instruction is cleared for public release and is available electronically only via Department of the Navy Issuances Web site, <https://www.secnav.navy.mil/doni>

POLICY

1. Discussion. The Department of the Navy executes its MEFs to fulfill requirements in support of the SECNAV, the Chairman of the Joint Chiefs of Staff (CJCS), Chief of Naval Operations (CNO), and Commandant of the Marine Corps. DON MEFs also support national essential functions and DoD primary MEFs.

2. DON MEFs. The DON has functions that must be continued throughout, or resumed immediately after, a disruption of normal activities. Per reference (d), the following subparagraphs 2a through 2e contain the DON MEFs.

a. Provide advice, as appropriate, to the President, Congress, National Security Council, Homeland Security Council, Secretary of Defense, and CJCS.

b. Provide and employ naval forces capable of protecting and defending the homeland and national interests.

c. Maintain worldwide situational awareness of naval forces, including their activities, capabilities, capacity, and readiness.

d. Support international coordination and cooperation programs.

e. Support domestic emergency response programs.

3. Action

a. Every command and organization within the Navy will implement a COOP program unless their COOP planning is included by the next higher authority in their chain of command (e.g., parent command or immediate superior in command (ISIC)), or they do not have functions required to be maintained through the first 30 days after an event. If a command determines it does not have functions required to be maintained for the first 30 days after an event, a waiver request must be submitted to CNO N3N5. Navy commands and organizations should be knowledgeable of their parent command or ISIC's COOP program. COOP programs require the identification of MEFs and the development of COOP plans and procedures to provide continuity of MEFs under all circumstances across the spectrum of threats, disasters, or incidents. MEFs are the functions directly related to accomplishing an organization's general mission as set forth in statutory or executive charter. MEFs also refer to essential supporting activities that the organization must continue in a continuity activation, such as human resources management, security, and facilities management. Reference (e) provides guidance and direction in the process for the identification and periodic review and verification of MEFs. COOP program and planning requirements for DON Components are specified in enclosure (3).

b. COOP plans must be comprehensive and executable with or without warning. Plans must also be flexible enough to enable contingency response from designated and contingency sites. Phased changes to site locations may also be required as a broad range of contingencies are addressed.

c. COOP plans must ensure the performance of MEFs during any emergency for up to 30 days or until normal operations can be resumed. The capability to perform MEFs at alternate sites must be fully operational as soon as possible, but no later than 12 hours after COOP activation.

d. Risk management must be used to determine the allocation of limited resources to meet continuity objectives and support the ability to perform MEFs.

e. COOP plans should make use of information technology (IT) solutions to provide information to leaders and other users, facilitate decision making, and enable the issuance of orders and direction. Technology, information systems (IS), and networks must be interoperable, robust, reliable, and resilient.

f. Continuity programs must be under the management of a senior official in the organization who is accountable to the commander, commanding officer, or officer in charge.

g. Continuity programs will ensure all personnel are trained on the organization's COOP plan at least annually. The COOP plan will be exercised on an annual basis.

h. COOP plans should be self-assessed using the COOP plan assessment benchmarks available in enclosure (4).

i. Per references (e), (f), and (g), DON critical infrastructure and emergency management require proactive actions to identify potential vulnerabilities and make risk based determinations. COOP planning is one element of the risk management program and is required for all DON critical infrastructure.

RESPONSIBILITIES

1. CNO N3N5 is responsible for the oversight, management, training, readiness, and compliance of Navy COOP programs and must:
 - a. exercise overall responsibility for the development, implementation, and management of Navy COOP policy and program direction;
 - b. ensure Navy COOP guidance, policies, plans, and procedures are consistent with directives from the President, Office of the Secretary of Defense, Department of Homeland Defense, Federal Emergency Management Agency, SECNAV, and CJCS;
 - c. ensure the COOP program is integrated and synchronized with readiness and mission assurance related programs;
 - d. assist echelon 2 commands and activities in developing their COOP plans;
 - e. conduct an annual review of the Navy COOP Program;
 - f. prepare, coordinate, validate, and maintain the Navy Headquarters COOP Plan;
 - g. ensure the Navy Headquarters COOP Plan supports Office of the Secretary of Defense, SECNAV, CJCS and CNO requirements;
 - h. forecast and establish budgetary requirements that support the Navy Headquarters COOP Plan;
 - i. plan, conduct, test, and assess Navy Headquarters COOP Plan exercises at least annually (these may be tabletop, functional, or full-scale exercises);
 - j. establish policy and provide guidance for identifying, storing, protecting, and maintaining Navy Headquarters COOP Plan emergency files, essential records, materials, and databases required to execute Navy Headquarters MEFs;
 - k. maintain an automated or manual Navy Headquarters COOP emergency relocation roster and alert and notification system, and conduct quarterly tests of the Navy Headquarters COOP alert and notification system; and
 - l. develop a multi-year continuity strategy and program management plan for obtaining and maintaining assets and resources in support of the Defense Continuity Program.

2. All Navy commands, organizations, and units must:
 - a. implement the requirements of this issuance; and
 - b. ensure COOP plans incorporate their component MEFs as the basis for their continuity planning, preparation, and execution.

COOP PROGRAM MINIMUM REQUIREMENTS

1. COOP programs and plans will, as a minimum, include the elements and requirements in subparagraphs 1a through 1o, per reference (h).

a. Program Management. Leadership, staff, communications, technology and facilities.

(1) Address COOP actions in four phases: readiness and preparedness, activation, continuity operations, and reconstitution.

(2) Recognize, endeavor to assist, and take advantage of parallel COOP processes that occur in other Federal Components and civil Government.

(3) Ensure assigned units develop a COOP plan to ensure their continuity, and that it supports their ISIC or parent command's COOP requirements. Tenants with MEFs should share and coordinate their COOP plans with the installation COOP planning officer or emergency manager to ensure that COOP plan assistance and support required from the installation is sufficiently coordinated.

(4) Ensure units assigned to support a unified combatant command properly support that command's COOP plans.

(5) Ensure COOP plans are structured to be able to perform MEFs in an all-hazard environment.

(6) Review COOP plans at least every 2 years and update as required.

(7) Establish a system of metrics to evaluate continuity requirements and certify program readiness.

(8) Conduct annual COOP plan self-assessment per enclosure (4).

b. Risk Management. Apply a risk-based framework across all continuity efforts to identify and assess potential hazards, determine what levels of risk are acceptable, and prioritize the allocation of resources per reference (i).

c. Budgeting and Acquisition of Resources

(1) Document and report all costs required to acquire, operate, and maintain COOP-related capabilities and facilities for the four COOP phases to the appropriate higher-level COOP office of primary responsibility (OPR). Documentation of costs should include operations and maintenance expenses that are associated with COOP capabilities.

(2) Develop procedures for expending funds, executing contingency contracts, and emergency procurement during COOP events.

(3) Include COOP funding in the organization's annual budget submission if applicable. Identify and justify estimates through prescribed budget exhibits and appropriate informational elements.

d. Essential Functions. Identify and prioritize MEFs and provide supporting justification (e.g., constitutional, legislative, presidential). Establish the priority of each function by examining the consequences of the nonperformance of those functions and plan to defer lower priority functions during a crisis. Prioritization will also guide MEF reconstitution operations. MEFs that require continuous performance or very rapid restoration following a disruption will likely require more robust backup systems, redundancies, and resiliencies than MEFs that may be recovered after a few days.

e. Orders of Succession. Establish and maintain orders of succession to key positions, and provide guidance and procedures to ensure the smooth transition of succession. Planning provisions should ensure the appropriate level of training and equipping for key personnel identified in the order of succession. General orders of succession guidelines are listed in subparagraphs 1e(1) through 1e(6) below.

(1) Identify orders of succession at least three positions deep for key leadership positions.

(2) Include designated officials assigned to devolution staffs, where applicable.

(3) Use geographically dispersed successors, where feasible.

(4) Describe orders of succession by positions or titles of individuals holding those offices.

(5) Obtain legal sufficiency reviews by the organization's legal counsel for original orders of succession determinations and as changes occur.

(6) Include orders of succession as essential files, with copies accessible or available at both the primary and alternate sites.

f. Delegations of Authority. Identify and document appropriate delegations of authority required to ensure continued, uninterrupted MEFs performance during and after a COOP event. Delegations of authority, like orders of succession, take effect when normal channels of direction are disrupted, and terminate when these channels have resumed, particularly in a devolution scenario. Organizations should identify the individuals to whom authorities are delegated by position title and not by name. However, individuals should be trained, qualified, and certified to execute authorities that may be delegated to them, as necessary. Delegations of authority:

- (1) are included as essential records;
- (2) are written per applicable statutes and regulations ensuring that the organization's MEFs are performed;
- (3) identify explicitly the authority of an official to re-delegate functions and activities, as appropriate;
- (4) describe the legal limits of and any exceptions to the authority and accountability for delegated officials; and
- (5) define the circumstances, to include a devolution situation if applicable, under which delegations of authorities would take effect and would be terminated.

g. Continuity Facilities. Identify at least one continuity facility (taking into account established distance criteria based on all-hazards analysis) from the main operating location of the respective organization. The term "continuity facilities" is comprehensive, referring to both alternate and devolution sites, as well as work arrangements such as telework and mobile work concepts. When considering continuity facilities, COOP planners should ensure:

- (1) sites are reachable and available during the full spectrum of hazards and emergencies;
- (2) sites have sufficient capability and supporting infrastructure, and can be fully operational within 12 hours of notification to activate the alternate site and commence MEF performance;
- (3) site considerations include distance from the threat area, vulnerability of relocation routes, and physical security including perimeter, access, billeting, internal functions, and networks and communications commensurate with the performance of essential functions;
- (4) transportation guidance and information is provided for individuals deploying to alternate locations; and
- (5) sustenance provisions (i.e., food and water) necessary to support relocation personnel for up to 30 days are identified and available.

h. Continuity Communications and IS. COOP plans must specify and prioritize the communications and IT systems required to perform each MEF.

(1) Continuity Communications. COOP plans must identify the emergency communications systems used by key leaders and other select continuity personnel while in transit and at the alternate sites. Systems to consider include those in subparagraphs 1h(1)(a) and 1h(1)(b) below.

(a) Government Emergency Telecommunications Service and Wireless Priority Service. COOP plans should identify continuity positions that require Government Emergency Telecommunications Service and Wireless Priority Service.

(b) Residential and mobile secure communications (e.g., DoD Mobility Classified Capability device) for senior leadership.

(2) Cyber - COOP Framework. COOP plans must identify the criticality and priority of IS required to perform essential functions and recognize cyber resiliency as an integral contingency measure. Furthermore, COOP planning must address the use of primary and alternate systems for the performance of essential functions. Reference (j) directs DoD to apply resilience to these resources and to implement a multi-tiered cybersecurity risk management process as described in National Institute of Standards and Technology Special Publication (NIST) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, and to develop IS contingency plans and conduct exercises to recover IS services following an emergency or IS disruption using guidance found in NIST Special Publication 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems. IS contingency plans provide key information needed for system recovery, including roles and responsibilities; inventory information; assessment procedures; detailed recovery procedures; and testing procedures for a system. For commands using the Navy Marine Corps Intranet, the IS contingency plan is maintained by the program office. COOP planners will:

(a) identify communications and networks ISs, control systems, secure and non-secure voice, data, and video that support essential functions and essential records;

(b) ensure essential systems and records at alternate sites are operational to support MEFs within required time frames; and

(c) identify and test IT systems and control systems per reference (g).

(3) Alternate Systems. These should include other methods, such as the use of voice, instead of data, and the use of data, instead of video. Alternate methods, which are not dependent on internet protocol-based IT systems, should be identified for the performance of essential functions in the case of a degraded cyberspace environment. Planning must also consider the use of alternate networks, e.g., classified network, should an unclassified network become disrupted.

i. Telework, Mobile Work, and Directed Work Locations. There is a direct relationship between COOP and telework. The two programs share the basic objective of performing and maintaining an organization's functions from an alternative location. Telework can assist sustainment of essential functions during a change to the normal operating status, such as during winter storms or a pandemic influenza event, however, telework may not be viable for continuing essential functions during all events (e.g., cyber events, mass power outage). If an

organization plans to utilize telework to continue essential functions, it must be documented in its continuity plan. When using telework as a primary or back-up continuity procedure, commands must adhere to reference (k) and provide protection of the information and ISs used during telework activities according to government standards.

j. Essential Records Management. Essential records refer to ISs technology, applications, infrastructure, electronic and hardcopy documents, references, and records needed to support the continued performance of essential functions during a continuity activation. They also include those records essential to protect the legal and financial rights of the Government and of the individuals directly affected by its activities. Appendix H of reference (l) sets forth the objectives and guidelines of the DON essential records program. This program is the means by which records that are needed to support COOP plans and procedures are identified, stored, and made accessible in a COOP situation. Planning should address procedures for routine backup and duplication of essential records. Essential records can be pre-staged at alternate facilities or maintained on networks with replicated storage sites. The program should be reviewed at least annually to determine its effectiveness and to ensure it is taking advantage of technological advances.

k. Human Resources and Personnel Accountability. An emergency response plan must ensure all employees (deploying and non-deploying) understand their role(s) during an emergency to include evacuation and shelter-in-place plans. In supporting the human capital needs of the continuity program, the continuity plan should account for all of the organization's human capital resources.

(1) Develop and implement a process to identify, document, communicate with, and train continuity and non-continuity personnel on their responsibilities.

(2) Safeguard documents per personally identifiable information and other DoD guidelines.

(3) Provide guidance to continuity personnel on individual preparedness measures to ensure rapid response to any local or national emergency per established emergency management planning.

(4) Implement a process to communicate the building's and organization's operating status to all of the organization's personnel.

(5) Implement a process to account for all staff in an emergency event as required in reference (d).

(6) Identify a human resource staff member to work with the organization's continuity planning officer to aid in the development of continuity plans.

(7) Implement a process to communicate guidance on pay, leave, staff, and other human resource issues to managers and personnel to help continue essential functions during any local or national emergency.

(8) Ensure appropriate language in contracts for contractors who are part of the continuity staff that legally binds and defines the contractors' responsibilities and level of participation during a continuity event.

l. Test, Training, and Exercise (TT&E) Program. DON organizations must plan, conduct, and document annual TT&E events to prepare for all-hazards continuity emergencies and disasters, identify deficiencies, and demonstrate the viability of their continuity plans and programs.

(1) Develop, update, and maintain a COOP TT&E plan. This may be integrated into an organization-wide TT&E plan, but COOP training and exercises must be clearly visible.

(2) Maintain COOP readiness of all individuals assigned emergency relocation group positions, and ensure their ability to perform MEFs in an all-hazard environment, per reference (b) with a developed training and exercise program.

(3) Test alert, notification, deployment procedures, operations, and support capabilities at alternate facilities annually. Exercises should simulate a cyber-degraded environment to aid in prioritizing ISs and developing necessary tactics, techniques, and procedures.

(4) Publish a corrective action plan following each exercise with issues entered into the organization's lessons learned (LL) database for resolution utilizing the organization's LL process and procedures. LL will be forwarded to the ISIC for improvement in other COOP plans. Incorporate LL from exercises and tests into the plan, as appropriate, and distribute both after action report and corrective action plan to appropriate internal COOP personnel and command leadership to allow necessary modifications and updates to COOP plans.

(5) Ensure COOP training addresses roles and responsibilities for deploying and non-deploying employees; work options and relocation procedures for non-deploying personnel; available support for family members of DON employees; alert, notification, and evacuation procedures; emergency contacts; security considerations, and drive-away kit requirements.

(6) Conduct and document annual COOP training and alternate site orientation for all personnel assigned. The COOP planning officer is responsible for tracking and documenting COOP training and alternate site orientation.

m. Devolution of Command and Control. Provide direction and guidance for units to establish devolution procedures, i.e., the transfer of MEFs in conjunction with related delegations of authority to execute such MEFs from the primary operating team to another organization,

command, or facility for an extended period of time until the primary team can re-establish command and control. Plans will include the establishment of essential memorandums of agreement, training, and equipping to support devolution.

n. Reconstitution Operations. Designate a reconstitution manager who will coordinate the development of post-event reconstitution procedures that allow for recovery from a catastrophic emergency and resumption of normal operations in coordination with facility and personnel management offices. COOP plans should include information essential to their reconstitution efforts including identification of:

(1) personnel, systems, communications, IT, office and conference space, and other capabilities required to re-establish normal operations;

(2) organizations responsible for providing reconstitution support to the Component (e.g., Washington Headquarters Services, General Services Administration) and any additional vendors and contract vehicles necessary to obtain essential services for reconstitution; and

(3) process to identify and incorporate LL into reconstitution planning and execution.

o. Continuity Plan Operational Phases and Implementation

(1) Continuity Operational Phases. Continuity plans within the DON will address the four operational phases of plan implementation as outlined in subparagraphs 1o(1)(a) through 1o(1)(d) below.

(a) Readiness and Preparedness. This phase includes all organization continuity readiness and preparedness activities including the development, review, and revision of plans, TT&E, and risk management.

(b) Activation. This phase includes the activation of plans, procedures, checklists, and schedules for the continuation of essential functions at alternate or devolution sites as well as for the personnel, essential records and databases, and equipment involved with these functions. This may include activation of supporting plans such as information operations disaster recovery plans, IS contingency plans, and building occupant emergency plans.

(c) Continuity Operations. This phase includes the activities listed in subparagraphs 1o(c)1 through 1o(c)5 to continue essential functions.

1. Accounting for all organization personnel.

2. Reporting on operational capabilities to ISIC.

3. Performing essential functions.

4. Establishing communications with supporting and supported organizations, customers, and stakeholders.

5. Preparing for the reconstitution of the organization.

(d) Reconstitution. This phase includes the personnel and facility-related actions required to resume full normal operations at the normal facility, another temporary facility, or a new permanent facility with the required staff and resources.

(2) Plan Implementation

(a) Planning should consider the challenges posed by extended events (e.g., pandemic influenza) that occur in a repetitious manner and cannot be addressed by traditional COOP responses.

(b) Validate or update and reissue plans every 2 years or more frequently as changes warrant, and provide a copy to the ISIC.

(c) Ensure civilian employee position descriptions and contractors' statements of work identify requirements as emergency relocation group team members with COOP responsibilities.

(d) Ensure security provisions and procedures for personnel, physical, operational, and information security are addressed and integrated into COOP planning and execution.

(e) Identify those positions within the organization that have the authority to activate the COOP plan.

(f) Apply security classification guidance to COOP plans and documents, per reference (m).

(g) Incorporate operations security into COOP execution and into exercise planning, implementation, and evaluation.

(h) Coordinate with the alternate facilities to ensure deploying personnel are cleared to enter the facility during the COOP event.

(i) Commands in the National Capital Region which are affected by continuity of government levels should identify relevant continuity of government requirements in their COOP plans.

2. Each command will have an office designated as the OPR for COOP, and appoint a continuity planning officer to serve as the point of contact for all COOP planning issues for the organization and subordinate elements, as well as higher echelons. OPR and continuity planning officer status information will be updated annually (or more frequently if changes occur) and provided to the ISIC to ensure dissemination of the latest directives and information.
3. Publish COOP guidance to ensure all levels of command effectively implement the COOP program and, if needed, develop their own instruction to supplement this instruction.
4. Establish methods to track the availability and readiness of all resources designated for use during all phases of COOP operations.

COOP PLAN ASSESSMENT BENCHMARKS

1. Purpose. These benchmarks are derived from reference (n) and address communications, facilities, IT, trained personnel, and other assets necessary to conduct MEFs and supporting activities. They also address specific activities that must be conducted in order to perform organizational mission essential tasks in support of assigned MEFs, and assess the ability of the DoD Component's MEFs to continue under all and across a wide range of potential emergencies, including localized acts of nature, accidents, and technological and attack-related emergencies.

2. Benchmarks

<u>Number</u>	<u>Category</u>	<u>Benchmark</u>
COOP-01	Program, Plans and Procedures	<p>Organizations must develop, coordinate, maintain, and validate continuity program and plans. Continuity plans must be reviewed every 2 years and updated, if necessary. Plans and procedures should provide clear objectives and instructions and must be executable with or without warning and during duty or non-duty hours.</p> <ul style="list-style-type: none">• Is a COOP planning officer designated in writing?• Do continuity plans, procedures, objectives, and requirements provide for the continued performance of an organization's MEFs under all circumstances?• Does the COOP plan address the following four operational phases?<ul style="list-style-type: none">• Readiness and preparedness?• Activation?• Continuity operations?• Reconstitution?• Does the plan identify interdependencies with other organizations, both within and outside the DoD?• Are operations security requirements integrated into the plan?• Can the plan be executed with or without warning?• Has a copy of the COOP plan and COOP point of contact been provided to the ISIC?• Is the COOP plan reviewed and updated at least every 2 years? <p><u>Best Practice:</u></p> <ul style="list-style-type: none">• References (b) and (e) provide checklists and templates for the development of a COOP program and plan.

COOP-02	Risk Management	<p>Risk management considerations must inform readiness decisions.</p> <ul style="list-style-type: none"> • How were the consequences of the non-performance of identified MEFs examined to determine criticality? • Has an impact or mission analysis been conducted to identify essential function relationships, interdependencies, time sensitivities, threats and vulnerabilities, that impact and support the performance of the MEFs?
COOP-03	Budgeting and Acquisition of Resources	<p>Ensure that continuity programs are supported by assets and resources, necessary for the development, operation, and maintenance of facilities, interoperable communications, and transportation capabilities.</p> <ul style="list-style-type: none"> • Does the budgeting and acquisition process ensure critical continuity resources are available to continue performing the agency's essential functions before, during, and after a continuity event?
COOP-04	MEFs and Essential Supporting Activities	<p>Responsible commanders must identify core requirements as the first step in continuity plan development. Core requirements include the identification of MEFs.</p> <ul style="list-style-type: none"> • Are MEFs identified and prioritized to support COOP planning and execution? (command and control; command decisions and strategies; crisis communications including alerts and notifications; crisis data storage, retrieval, and security; legal obligations; fiscal and contractual obligations; personnel; and critical support to or from other DoD Components?) • Are interdependencies needed to perform MEFs identified? <p><u>Best Practice:</u></p> <ul style="list-style-type: none"> • Identify installation support to critical assets and tenant continuity plans.
COOP-05	Orders of Succession	<p>Continuity planning should establish orders of succession.</p> <ul style="list-style-type: none"> • Is there a documented clear line of succession in the absence of leadership during the course of any emergency to enable an orderly and predefined transition of leadership within the organization per applicable laws and directives? • Are orders of successions established with at least three positions identified in the line of succession, to include a geographically dispersed successor, where feasible? • Are orders of succession identified by titles and positions, rather than by names of individuals holding those offices?

COOP-06	Delegations of Authority	<p>Continuity planning should establish pre-planned and emergency delegations of authority.</p> <ul style="list-style-type: none">• Is there a documented delegation of authority to make policy determinations and decisions for key agency leadership positions at the HQ, regional, field, satellite, and other levels and agency locations, as appropriate, to ensure a rapid response to any emergency and to minimize disruptions that require continuity implementation?• Are key agency officials informed of and trained on the agency delegations of authority so that the agency can transfer leadership authority in an orderly manner, when applicable, during a response to any emergency?• Has delegation of authority been coordinated with the appropriate legal staff to ensure legal sufficiency?
---------	--------------------------	--

COOP-07	Continuity Facilities	<p>Continuity planning should include the identification of continuity facilities for component use during continuity threats or events. Site selection must consider ISs and networks, geographical dispersion, physical security, and maximize colocation and dual-use facilities with a focus on risk mitigation. Continuity facilities include relocation facilities as well as devolution sites.</p> <ul style="list-style-type: none">• Are continuity facilities identified to provide survivable protection and sustain continued, enduring operations under any circumstance for a minimum of 30 days?• Can continuity facilities be fully operational within 12 hours?• Is a process established to notify and coordinate activation of the continuity location(s)?• Are the following considerations part of the continuity facility selection process?<ul style="list-style-type: none">• Administrative support and management?• Coordination of clearances and access?• Logistics, billeting?• Alternate usages of existing facilities?• Virtual office options including telework?• Geographic dispersion?• ISs and networks?• Physical security?• Contractor support, if required?• Is equipment prepositioned at the continuity facility adequate to continue operations?• Is there a memorandum of agreement?• Do non-relocation staff members have contact information for the continuity facility?• Have critical documents (essential records) been pre-positioned?
---------	-----------------------	---

COOP-08	Continuity Communications	<p>Continuity planning must address IT and communications support to continuity operations.</p> <ul style="list-style-type: none"> • Are the effective continuity communications systems that support mission essential connectivity, under all conditions, among key government leadership, internal elements, other agencies, critical customers, and the public identified and available? • Does the plan contain information that indicates relevant communications and network connectivity at alternate operating facilities are commensurate with the execution requirements of the MEFs? Plan should identify mission-critical information and technological and communication systems, to include services, applications and Web sites that are essential to performance of organizational MEF and essential supporting activities. Plan should detail how organization responds to the effects of degradation of DoD information network capabilities. Plan is informed by component-level IS contingency plans aimed at recovery of IS services following an emergency or IS disruption. • Is there an alert and notification system or procedures in place for notifying relocation staff?
COOP-09	Essential Records Management	<p>Continuity planning must provide for the identification, storage, protection, and availability for use at relocation sites of the essential records, materiel, and databases required to execute MEFs. Pre-positioning and storage procedures should be enduring, survivable, and redundant.</p> <ul style="list-style-type: none"> • Are all essential records needed to continue essential functions and to resume normal operations throughout all phases of a continuity event identified, maintained, survivable, and accessible from the continuity facility? • Are essential records programs and capabilities tested and updated as required? • Are continuity personnel trained and exercised on essential records access and programs?

COOP-10	Human Resources	<p>Continuity planning must include training of continuity staffs and provide orientation and awareness training.</p> <ul style="list-style-type: none">• Are continuity leadership and staff identified?<ul style="list-style-type: none">• Have continuity leadership and staff acknowledged and accepted their continuity role (e.g., through position descriptions, contract language, or other formal means)?• Has a telework policy been established?• Has an emergency relocation staff been identified?• Does the plan outline procedures for monitoring an approaching pandemic, distributing information to employees, enacting pre-pandemic mitigation strategies, as well as the decision-making process that would lead to activation of the plan?
---------	-----------------	--

COOP-11	TT&E Program	<p>Responsible commanders should integrate continuity-related functions and activities into operations and exercises to ensure that MEFs can be performed under all circumstances across the spectrum of threats.</p> <ul style="list-style-type: none"> • Is there a documented or commonly understood and practiced continuity testing, training, and exercise program established that demonstrates, assesses, and improves the ability to execute the continuity program, plans, and procedures and perform essential functions during all continuity events? • Is the COOP plan exercised annually? Be prepared to provide a written after action report that captures the specifics and findings of the exercise. <ul style="list-style-type: none"> • The after action report is to be signed by a senior tasked with oversight of continuity or the senior-most exercise participant. • Is the TT&E program supported by a corrective action program? • In the past year, has orientation and awareness training been conducted for continuity staff? <ul style="list-style-type: none"> • Are records of participation maintained? • Is cybersecurity incorporated into the annual continuity exercise? <ul style="list-style-type: none"> • Is the exercise planned in coordination with the organization's IT service providers? • Are continuity communications systems tested and updated as required? • Are these testing results identified with a corrective action plan? <p><u>Best Practice:</u></p> <ul style="list-style-type: none"> • Cybersecurity may be incorporated into annual exercises in a variety of ways including, simulated system outages, denied access to essential records, and emergency relocation group discussions and table top exercises focused on cybersecurity.
COOP-12	Devolution of Command and Control	<p>Continuity planning should establish devolutions of authority for essential functions and key positions.</p> <ul style="list-style-type: none"> • Is there an established devolution plan or procedures? • Do the devolution plan or procedures address personnel, planning, resource, and training considerations needed to transfer agency essential functions and leadership authorities away from the primary facility or facilities to a continuity location?

COOP-13	Reconstitution Operations	<p>Provide for reconstitution capabilities that allow for recovery from an emergency and resumption of normal operations.</p> <ul style="list-style-type: none">• Does the COOP plan address a reconstitution plan and procedures?• Has a reconstitution manager been assigned?
---------	---------------------------	--